33. A method of preventing replay attacks comprising:

defining a first private-public key pair comprising a first private key and a first public key;

providing the first public key to a cryptographic processing system;

defining a second private-public key pair comprising a second private key and a second public key;

performing a first secure code update using the first private-public key pair to provide the second public key to the cryptographic processing system; and

performing a second secure code update using the second private-public key pair.

34. The method of claim 33 wherein performing the second secure code update comprises providing new code and a new function table for the cryptographic processing system.

35. The method of claim 34 comprising encrypting the new code and the function table and storing the encrypted new code and function table in a data memory associated with the cryptographic processing system.

36. The method of claim 35 wherein the data memory comprises a flash memory located external to the cryptographic processing system.

37. The method of claim 33 comprising encrypting the second public key before it is stored in a data memory associated with the cryptographic processing system.

38. The method of claim 37 wherein the data memory comprises a flash memory located external to the cryptographic processing system.

39. The method of claim 33 wherein performing the first secure code update comprises updating a secure code descriptor.

* * * * *